Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	

To: The Commission

PETITION FOR RECONSIDERATION

Oracle[1] hereby petitions the Federal Communications Commission ("Commission" or "FCC") for reconsideration of the Report and Order ("*Order*") in the above-referenced proceeding.[2] The *Order* correctly recognizes that protecting consumer privacy online is "fundamental,"[3] but completely undermines that goal by handing Google the market to the obvious detriment of consumers. If the *Order* goes into effect, broadband internet access service ("BIAS") providers (*i.e.*, Internet Service Providers or "ISPs") will face new restrictions and

[1] Oracle offers an integrated array of applications, databases, servers, storage, and cloud technologies to empower modern business. Oracle provides a wide choice of software, systems, and cloud deployment models – including public, on-premises, and hybrid clouds – to ensure that technology flexes to the unique needs of a business. More than 420,000 customers across 145 countries have harnessed Oracle technology to accelerate their digital transformation.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, WC Docket No. 16-106, FCC 16-148 (rel. Nov. 2, 2016) ("*Order*").

All references to "Comments" in this petition are to comments filed in WC Docket 16-106 on or about May 27, 2016; references to "Reply Comments" are to reply comments filed in WC Docket 16-106 on or about July 6, 2016.

[3] *Id.* ¶ 1.

requirements that do not apply to Google or other providers of other online services ("edge providers").[4]

ISP-specific privacy rules that depart from the privacy approach of the Federal Trade Commission ("FTC") (which remains applicable to ISPs' edge provider competitors) will hurt competition.[5] The corresponding harm to consumers is clear from an examination of the *Order*'s benefits for Google. Google already has the ability to track virtually every movement of a consumer's day through an Android phone or tablet.[6] It has created a proprietary Android world to derive substantial economic benefit from advertising and – perhaps even more importantly – obtain access to huge amounts of personal data through search, location tracking, and other activities. The Android license required to be obtained by OEMs as a condition precedent to manufacture includes significant demands that severely constrain developers. Moreover, because Google controls the distribution mechanism for apps, competition and consumers are further harmed. Google is largely outside the FCC's authority,[7] and now the Commission has handed Google a new regulatory gift in the form of imbalanced burdens on ISPs.

---

[4] Unlike every other player of the internet ecosystem, under the Commission's new rules, ISPs must treat web browsing and application usage history as sensitive, including by obtaining opt-in approval to use such information for general first-party marketing. *Id.* ¶¶ 181, 192, 199.

[5] *See, e.g.*, Charter Reply Comments at 19 ("[R]egulating ISPs' use and disclosure of customer information more strictly than other entities in the online ecosystem … would tilt the playing field in favor of Facebook, Google, and other edge providers, enabling them to continue to dominate the market."); International Center for Law and Economics Comments at 3 (stating that the Commission's proposed rules "are designed to keep ISPs from competing with edge providers like Google, Facebook, and Netflix."); Roslyn Layton Comments at 5-12 (noting online advertising revenue is increasingly concentrated in one company, Google").

[6] *See, e.g.*, Amy Kraft, *Google is spying on K-12 students, privacy advocates warn*, CBS News (Dec. 29, 2015), http://cbsn.ws/1OwMCj2; *Mission Creep-y: Google Is Quietly Becoming One of the Nation's Most Powerful Political Forces While Expanding Its Information-Collection Empire*, Public Citizen, Nov. 13, 2014, http://bit.ly/1qRXib0; John Timmer, *EU seeks Street View picture purge*, Ars Technica, Feb. 26, 2010, http://bit.ly/2fWEytk.

[7] *See e.g.*, Statement of Commissioner Ajit Pai (dissenting), *Order* at 210 ("Pai Dissent") ("Nothing in these rules will stop edge providers from harvesting and monetizing your data, whether it's the websites you visit or the YouTube videos you watch or the emails you send or the search terms you enter on any of

These rules will create a chilling effect by giving "a clear competitive advantage to edge providers" that already dominate the digital advertising market.[8] If asymmetric regulation – and the marketplace imbalance it creates – ever is appropriate, it is inappropriate here where ISPs are not differently situated from the edge providers that dominate the online advertising market in any relevant respect. The Commission should reconsider the aspects of the *Order* that rely on this demonstrably flawed premise and ensure that ISPs are subject to the same privacy rules as their competitors.

I. THE *ORDER* IGNORES AND DRAMATICALLY UNDERSTATES THE ONLINE TRACKING CAPABILITIES OF GOOGLE AND OTHER EDGE PROVIDERS

The *Order* treats ISPs differently from edge providers based on the readily disproved notion that although "there are other participants in the Internet ecosystem that can also see and collect consumer data, … BIAS providers' gatekeeper position allows them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its content."[9] By contrast, according to the *Order*, "edge providers only see a slice of any given consumers Internet traffic."[10] The record, however, made clear that certain edge providers see far more than "only a slice of any given consumers Internet traffic."[11]

---

your devices."); *see also* Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, WC Docket No. 16-106, at 24-25 (filed May 27, 2016) ("Swire Paper"); Electronic Privacy Information Center ("EPIC") Comments at 16.

[8] Competitive Carrier Association Reply Comments at 32.

[9] *Id.* ¶ 30.

[10] *Id.*

[11] *See* Dissenting Statement of Commissioner Michael O'Rielly, *Order* at 214 (observing that the "ridiculous notion" that BIAS providers "see more information about their customers than edge providers … has been thoroughly debunked in the record") (citing Swire Paper at 24-25; EPIC Comments at 16; Comcast Comments at 26-34; Verizon Comments at 16-24).

Specifically, the *Order*'s flawed assertions about the internet ecosystem[12] neglect at least two key consumer information-harvesting edge provider services that substantially alter the privacy landscape: operating systems ("OS") and web browsers.[13] And, some of the largest edge providers provide more than one service and function – a fact that the *Order* largely ignores – the combination of which can yield incredibly detailed profiles about consumers. These services offer their providers as much, or likely more, access to information such as web browsing history compared to the access of ISPs.

The example of Google definitively disproves the Commission's rationale for treating "ISPs differently from edge providers."[14] The *Order* observes that Google has third party tracking capabilities across more than 10 percent of the top one million websites,[15] but underestimates how Google combines and uses collected data to create full profiles of individuals.[16] For example, Google also makes available services through its domain,[17] and thus

---

[12] *See, e.g.*, *Order* ¶ 30 ("[O]nly three companies (Google, Facebook, and Twitter) have third party tracking capabilities across more than 10 percent of the top one million websites, and none of those have access to more than approximately 25 percent of web pages," in contrast to BIAS providers that see "100 percent of a customer's unencrypted Internet traffic."); *id.* ¶ 31 ("[U]sers have much more control over tracking by web third parties than over tracking by BIAS providers," including through "[a] range of browser extensions[.]"); *id.* ("Internet participants that see Domain Name System ("DNS") lookups see DNS lookups "only to their own domains (e.g., google.com, facebook.com, netflix.com)[.]").

[13] *See* EPIC Comments at 16 ("The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company."); Pai Dissent at 210 (noting that "any review of the headlines rebuts the FCC's assertion that edge providers only see a fraction of your data").

[14] *See* Pai Dissent at 210 ("[B]ecause the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a 'slice' of consumers' online data.").

[15] *See Order* ¶ 30. In fact, Google – through its DoubleClick and Google Analytics services – holds 80 percent market-share of third-party tracking services on the most popular, top-level domains. Datanyze, Analytics market share in the Datanyze Universe, https://www.datanyze.com/market-share/analytics (last visited Dec. 12, 2016).

[16] *See, e.g.*, Center for Digital Democracy, Paper, *Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers Center for Digital Democracy*,

has access to any DNS lookup from google.com or any other domain controlled by Google (*e.g.*, youtube.com). And, Google offers far more than just its website and has far more tracking capabilities than just on top websites.[18] In fact, Google is a major market player in online web search, social media applications, online video, OS, email, digital ads, over-the-top messaging, and web browsing.[19] Each of these services independently provides Google with significant access to consumer information; together they allow Google to compile complete and comprehensive profiles of scores of consumers.[20]

Further, every consumer with an Android device must use a Google Play ID to purchase apps through the Google Play store (formerly the Android Market), which comes pre-installed on Android devices.[21] This means that any app written for Android would require subscribers to share significant amounts of personal data with Android – *i.e.*, with Google. In addition to smartphones, Google is now bringing Android app capabilities to its Chromebook laptops, to newer TVs through Chromecast, directly to Android-based "smart TVs", watches, automobiles,

---

WC Docket No. 16-106, at 72-74 (filed May 23, 2016) (observing that Google links individuals across platforms and devices) ("CDD Paper").

[17] *See Order* ¶ 31.

[18] *See, e.g.*, Comcast Comments at 31 ("[N]on-ISPs that have affiliate relationships with many different types of Internet businesses are able to track users across multiple websites, apps, devices, services, and locations, and compile extensive and comprehensive consumer profiles across those platforms. Google is the most notable example of this.").

[19] *See* Swire Paper at Diagram 8-A.

[20] *See* Google, *Welcome to the Google Privacy Policy* (last modified Aug. 29, 2016) ("Google Privacy Policy"), https://www.google.com/policies/privacy ("We may combine personal information from one service with information, *including personal information*, from other Google services….") (emphasis added).

[21] Google in many instances has access to a consumer's name, address, phone number, and billing history. *See Order* ¶ 32 (stating that access to such information "gives ISPs a very unique, detailed and comprehensive view of their users that can be used to profile them in ways that are commercially lucrative").

and so much more – each device capable of collecting and tracking additional information from consumers.

Every time a consumer "wakes"[22] an Android device, the device sends and receives over 35 data requests. Among these requests, the device transmits to Google its (i) location, (ii) Google Play ID, and (iii) Mobile ID. In addition, Google's recent decision to link its DoubleClick data into its profiles exponentially expands Google's ability to aggregate specific consumer data in a way that is orders of magnitude more pervasive than other technology companies such as Oracle.[23] For example, one commenter told the Commission that "Google alone (with all its various data-grabbing applications) most likely collects, stores, and utilizes far more personal information than all the ISPs combined."[24]

Beyond Google's data collection capabilities through Android, Google's other services also allow it to collect a tremendous amount of data[25] – data which Google can combine across each platform and device a consumer uses to serve targeted advertisements.[26] Google's Chrome

---

[22] To "wake" an Android device is to turn on the display screen by, for example, tapping the power button.

[23] Julia Angwin, *Google has Quietly Dropped Ban on Personally Identifiable Web Tracking*, PROPUBLICA, Oct. 21, 2016, https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking (Having unilaterally dropped its policy against undertaking personally identifiable web tracking for DoubleClick, "Google could now, if it wished to, build a complete portrait of a user by name, based on everything they write in email, every website they visit and the searches they conduct.").

[24] *See* Free State Foundation Comments at 2; *see also* Comcast Comments at 31 ("[T]here can be little doubt that non-ISPs like Google, ad networks, data brokers, and the other entities analyzed [in the Swire Paper] have access to consumer information that far exceeds a stand-alone ISP's access to information.").

[25] Nick Statt, *Why Google's fancy new AI assistant is just called 'Google'*, THE VERGE, May 20, 2016, http://www.theverge.com/2016/5/20/11721278/google-ai-assistant-name-vs-alexa-siri ("[t]he number of things Google can't do is shrinking. Google knows your weekly calendar, your flight times, your dinner reservations, your music and TV and movie tastes, who your friends are, how often you talk to them and much, much more about your personal life.").

[26] *See, e.g.*, CDD Paper at 73 (noting that Google "provides a number of programmatic data-targeting services for video," among other services); Google Privacy Policy ("When used in conjunction with our advertising services, such as those using the DoubleClick cookie, *Google Analytics information is linked*

web browser allows it access to full URLs a user visits and the specific content of those URLs, even when traffic is encrypted.[27] Google's Gmail offers it the potential ability to see "information about all facets of [consumers'] life … such as their thoughts, ideas, goals, fears, etc.," and "[t]his information is not only current, but may reflect a user's past or future."[28]

Google's practices, of course, fall outside the scope of the FCC's authority, but the Commission's failure to fully take into account the detailed record of Google's massive information-gathering capabilities is a disservice to consumers and must be corrected. That correction should begin by eliminating the asymmetrical treatment of ISPs that hamstrings them as competitors.

II. ANDROID USERS – AND PARTICULARLY GMAIL USERS – HAVE THE SAME LIMITED ABILITY TO CHOOSE WHETHER TO REVEAL INFORMATION TO GOOGLE AS TO THEIR ISPS

The *Order* also attempts to draw a false distinction between consumers' choices and expectations with respect to their ISPs versus their edge providers and operating systems. These claims warrant reconsideration, as they completely ignore the realities of the online ecosystem with respect to certain dominant edge providers, such as Google. Just as with their ISPs, consumers have little choice regarding whether to reveal personal information to Google[29] and

---

… *using Google technology, with information about visits to multiple sites*") (emphasis added); *New digital innovations to close the loop for advertisers*; Google Inside AdWords (Sept. 25, 2016), https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html ("The final loop to close is the one across all the devices people use – phones, tablets, laptops and everything in between. Today, we're introducing cross-device remarketing for Google Display Network and DoubleClick Bid Manager to help you reach the same user across devices, apps, and sites.") (emphasis omitted).

[27] *See* Swire Paper at 90.

[28] *Id.* at 59

[29] An Android device may come with, for example, a default web browser, messaging app, webmail service, app store, and more, all tied directly into Google's Android OS.

costs to switch between OS providers are substantial,[30] making a switch an impractical option to avoid revealing information – perhaps even more so than a switch between ISPs.

Importantly, even a switch among competing edge providers' applications, or a switch to a different device manufacturer, may leave a consumer captive to the exact same operating system. In addition to Google itself, many manufacturers utilize the Android OS, meaning that switching devices often means staying within the Android sandbox.[31] Further, all but the most sophisticated Android users must use Google Play to download new apps – as described above, when a consumer must use Google Play, the consumer does not make a choice at all, let alone each time, whether or not to reveal information to Google upon downloading a new app or game. Nor do Gmail users decide each time they send or read an email whether or not to reveal information. Even if a consumer used no application other than Gmail, the consumer would be forced to reveal a significant amount of information to Google, captive to the provider despite privacy concerns in order to avoid losing access to years and years of archived email messages.[32]

---

[30] The *Order* asserts that "consumers have a choice in deciding each time whether to use—and thus reveal information—to an edge provider, such as a social network or a search engine, whereas that is not an option with respect to their BIAS provider when using the service," and claims that ISPs' so-called gatekeeper position "is strengthened by high switching costs customers face when seeking a new service, which could deter customers from changing BIAS providers if they are unsatisfied [with] the providers' privacy policies." *Order* ¶ 36. Yet these same "high switching costs" exist for operating systems and similarly could deter customers from switching in the event of privacy concerns. To switch OS providers – again, practically speaking, switching from iOS to Android or vice versa for mobile devices – consumers first need to purchase a new device before then working to ensure that their contacts, photos and videos, apps, and more make it to the new device and the new system. As one reporter concluded based in part on his own experience, "[g]iven the headaches of switching, most people avoid it." *See* Vindu Goel, *How to Switch to iPhone From Android: Patience and Persistence*, NY TIMES, Apr. 6, 2016, http://www.nytimes.com/2016/04/07/technology/personaltech/how-to-switch-to-iphone-from-android-patience-and-persistence.html ("Switching phone operating systems should in theory be simple. First you transfer your data from the old phone to the new one. Then you reinstall your favorite apps. Finally you customize the setting for features like ring tones and notifications and learn the quirks of your new device…. But as I learned, many things can go wrong, and my experience is not unusual.").

[31] *See, e.g.*, Swire Paper at 76.

[32] They also may lose contact with friends and family who do not learn of their new email addresses.

Google's intrusive and ubiquitous reach far outweighs any reasonable consumer expectation of Android or any Android app. Moreover, even if the *Order* is correct that consumers paying a fee for broadband have no reason to expect that their service is being subsidized by ISP advertising revenue,[33] this same conclusion should hold true for customers who purchase a wireless device that includes a built-in operating system. The Commission cannot allow the *Order* to stand, when it hands a clear victory to Google by hamstringing ISPs while allowing Google to continue to engage in invasive data collection and aggregation techniques, bolstered by its tight control of the Android operating system.

[33] *See Order* ¶ 35 ("[C]ustomers generally pay a fee for their broadband service, and therefore do not have a reason to expect that their broadband service is being subsidized by advertising revenues as they do with other internet ecosystem participants.").

III. CONCLUSION

The *Order* relies on the flawed premise that ISPs are situated differently than edge providers and reaches the flawed conclusion that ISPs should be subject to a stricter privacy regime. This result ignores the expansive information collection capabilities of edge providers such as Google and harms consumers by magnifying, rather than reducing, a critical imbalance in the internet ecosystem. For this reason, the Commission should reconsider the *Order* and, at a minimum, subject ISPs to the same privacy regime as edge providers are subject to at the Federal Trade Commission.

Respectfully submitted,

ORACLE CORPORATION

By: */s/ Kenneth Glueck*

Kenneth Glueck
Senior Vice President
Office of CEO

Oracle Corporation
1015 15th St. NW, Suite 200
Washington, DC 20005
(202) 721-4815

December 21, 2016